<?xml version='1.0'?>

<PaymentInfo xmlns='http://example.org/paymentv2'>

<Name>John Smith</Name>

<CreditCard Limit='5,000' Currency='USD'>

<Number>

<EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'

Type='http://www.w3.org/2001/04/xmlenc#Content'>

<CipherData>

<CipherValue>A23B45C56</CipherValue>

</CipherData>

</EncryptedData>

</Number>

<Issuer>Example Bank</Issuer>

<Expiration>04/02</Expiration>

</CreditCard>

</PaymentInfo>

<EncryptedData Id='ED' xmlns='http://www.w3.org/2001/04/xmlenc#'>

<EncryptionMethod

Algorithm='http://www.w3.org/2001/04/xmlenc#aes128-cbc'/>

<ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>

<ds:RetrievalMethod URI='#EK'

Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>

<ds:KeyName>Sally Doe</ds:KeyName>

</ds:KeyInfo>

<CipherData><CipherValue>DEADBEEF</CipherValue></CipherData>

</EncryptedData>

<KeyInfo>

<X509Data> <!-- two pointers to certificate-A -->

<X509IssuerSerial>

<X509IssuerName>CN=TAMURA Kent, OU=TRL, O=IBM,

L=Yamato-shi, ST=Kanagawa, C=JP</X509IssuerName>

<X509SerialNumber>12345678</X509SerialNumber>

</X509IssuerSerial>

<X509SKI>31d97bd7</X509SKI>

</X509Data>

<X509Data><!-- single pointer to certificate-B -->

<X509SubjectName>Subject of Certificate B</X509SubjectName>

</X509Data>

<X509Data> <!-- certificate chain -->

<!--Signer cert, issuer CN=arbolCA,OU=FVT,O=IBM,C=US, serial 4-->

<X509Certificate>MIICXTCCA..</X509Certificate>

<!-- Intermediate cert subject CN=arbolCA,OU=FVT,O=IBM,C=US

issuer CN=tootiseCA,OU=FVT,O=Bridgepoint,C=US -->

<X509Certificate>MIICPzCCA...</X509Certificate>

<!-- Root cert subject CN=tootiseCA,OU=FVT,O=Bridgepoint,C=US -->

<X509Certificate>MIICSTCCA...</X509Certificate>

</X509Data>

</KeyInfo>

<EncryptedKey Id='EK' xmlns='http://www.w3.org/2001/04/xmlenc#'>

<EncryptionMethod

Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1\_5"/>

<ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>

<ds:KeyName>John Smith</ds:KeyName>

</ds:KeyInfo>

<CipherData><CipherValue>xyzabc</CipherValue></CipherData>

<ReferenceList>

<DataReference URI='#ED'/>

</ReferenceList>

<CarriedKeyName>Sally Doe</CarriedKeyName>

</EncryptedKey>

<RSAKeyValue>

<Modulus>

xA7SEU+e0yQH5rm9kbCDN9o3aPIo7HbP7tX6WOocLZAtNfyxSZDU16ksL6W

jubafOqNEpcwR3RdFsT7bCqnXPBe5ELh5u4VEy19MzxkXRgrMvavzyBpVRg

BUwUlV5foK5hhmbktQhyNdy/6LpQRhDUDsTvK+g9Ucj47es9AQJ3U=

</Modulus>

<Exponent>AQAB</Exponent>

</RSAKeyValue>